UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,687	04/02/2004	Uwe Eckhardt	5800-00601	9738

53806 7590 04/28/2009

MEYERTONS, HOOD, KIVLIN, KOWERT & GOETZEL (AMD)
P.O. BOX 398
AUSTIN, TX 78767-0398

EXAMINER	
SAN JUAN, MARTINJERIKO P	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,687	ECKHARDT ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *February 25, 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-9,11,12,14-57,59-69 and 71-74* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-9,11,12,14-23,25-57,59-69 and 71-74* is/are rejected.

7)☒ Claim(s) *24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Remarks filed on February 25, 2009

Claims 1-3, 6-9, 11-12, 14-57, 59-69, and 71-74 are currently pending.

Response to Arguments

1. Applicant's arguments filed February 25, 2009 have been fully considered but they are not persuasive.

The Examiner respectfully disagrees that Edwards does not teach the limitation "wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a prioritization algorithm implemented on the single-purpose hardware." There is no positive definition of what the prioritization algorithm is. Furthermore, the limitation does not limit all the prioritization work to be performed solely by the single-purpose hardware, but rather, a certain prioritization algorithm is implemented on the single-purpose hardware. The Examiner is interpreting the prioritization algorithm to be the Hardware-based MAC component pulling packets from the higher priority queue before the remaining queues for encapsulation and transmission [Edwards 5: 0052 --In particular, transmit logic may be configured to pull packets exclusively from one queue, or the other, or to pull packets from both with a higher priority given to one of the queues.].

The Examiner respectfully disagrees that Edwards does not teach the limitation "wherein said data frame encapsulation and decapsulation is performed on a single purpose hardware of said WLAN chip without executing software-implemented

instructions of said driver software." Edwards in Figure 6 shows the Hardware-base MAC (24B) of Figure 4 comprising the encryption (42), decryption (50), and the checksum generator (44) engines. As previously state, the Examiner interprets encapsulation and decapsulation as encryption and decryption.

Regarding the Official Notice, the Examiner clarifies that the 802.11 defines the radio frequency is spread at 11 Mhz. The authority of this information is found on the 802.11 1999 Standard, Chapter 15. The Examiner agrees with the Applicant that "IEEE 802.11 defines a spectral mask wherein a signal is attenuated by at least 30 dB from its peak energy at ±11 MHz from the center frequency." As such, any device conforming to the 802.11 would have had some operation associated with 11 Mhz. [Specifically, there would have been a 11 Mhz chip clock to spread the energy out from the channel center in multiple of 11 Mhz.]

Allowable Subject Matter

1. Claim 24 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1-3, 6-9, 11-12, 16-20; 26-27, 29-32, 46-57, 59-61,69, and 71-74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Edwards et al. [US

2004/0059825 A1], hereinafter Edwards, and further in view of IEEE [IEEE 802.11 (1999)].

Regarding claim 1, Edwards teaches a method of performing encrypted IEEE 802.11 WLAN (Wireless Local Area Network) communication [Edwards 3: 0038], comprising the steps of:

operating driver software to perform a connection set-up for said encrypted WLAN communication [Edwards 4: 0045 --connection set-up is associated with authentication, and network management performed by the software-based MAC] [Edwards Fig 4: software-based MAC is part of driver in host computer.]; and operating a WLAN chip to perform data frame encapsulation and decapsulation during said encrypted WLAN communication [Edwards 4: --data frame encapsulation and decapsulation is associated with hardware-based MAC encryption and decryption.];

wherein said connection set-up is performed by executing software-implemented instructions of said driver software without exchanging intermediate data with said WLAN chip [Edwards Fig 4: Itm 24A --software-based MAC is part of driver in host computer.], wherein performing said connection set-up comprises exchanging exchanging of cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point [Edwards 6: 0059];

wherein said data frame encapsulation and decapsulation is performed on a single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software [Edwards Fig 4: Itm 24b], wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames

intended for said data frame encapsulation from driver software [Edwards 4: 0050 --Host may write packets directly into one or both of transmit queues, via the software-based MAC component running within the driver software executed by host CPU.]; and wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a prioritization algorithm implemented on the single-purpose hardware [Edwards 5: 0052 --transmit logic may be configured to pull packets exclusively from one queue or the other, or to pull packets from both queues with a higher priority given to one of the queues.].

Edwards does not explicitly teach wherein of performing said data frame encapsulation comprise calculating an integrity value appropriate for verifying integrity of one of the plurality of data frames once said data frame decapsulation is completed.

IEEE teaches a standard for wireless communication where performing said data frame encapsulation comprise calculating an integrity value appropriate for verifying integrity of one of the plurality of data frames once said data frame decapsulation is completed [IEEE 802.11 (1999): Chapter 8: --Note section 8.2.5, WEP ICV].

It would have been obvious to one of ordinary skilled in the art at the time of invention to incorporate the calculating of the integrity value when performing the data frame encapsulation as taught by the IEEE standard. The suggestion/motivation to combine would have been to incorporate aspects of the IEEE standard for compliance [Edwards 3: 0038].

With regard to dependent claim 2, Edwards in view of the IEEE teach the method of claim 1, wherein the step of performing said connection set-up comprises authenticating a WLAN station by another WLAN station and/or a WLAN authentication server [IEEE 802.11 (1999) Sec 5.4.3.1]

With regard to dependent claim 3, Edwards in view of the IEEE teach the method of claim 1, wherein the step of performing said connection set-up comprises associating a WLAN station with another WLAN station and/or a WLAN access point as WLAN communication counter-parts [IEEE 802.11 (1999) Sec 5.4.2.2].

With regard to dependent claim 6, Edwards in view of the IEEE teach the method of claim 1, wherein the step of obtaining the plurality of data frames comprises obtaining a plurality of data frames comprising cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises WEP].

With regard to dependent claim 7, Edwards in view of the IEEE teach the method of claim 6, therein said determining factor comprises a way in which a data frame intended for the data frame encapsulation is fragmented [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises More Frag].

With regard to dependent claim 8, Edwards in view of the IEEE teach the method of claim 6, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises WEP].

With regard to dependent claim 9, Edwards in view of the IEEE teach the method of

claim 6, wherein said determining factor comprises a cryptographic key suitable for encrypting a data frame [IEEE 802.11 (1999) Sec 8.2.5 --cryptographic key is derived from IV which is associated with WEP].

With regard to dependent claim 11, Edwards in view of the IEEE teach the method of claim 1, wherein the step of performing said data frame encapsulation comprises inserting a package number and/or sequence number into one of the plurality of data frames [IEEE 802.11 (1999) Sec 7.1.3.4].

With regard to dependent claim 12, Edwards in view of the IEEE teach the method of claim 1, wherein the step of performing said data frame encapsulation comprises encrypting at least part of one of the plurality of data frames [IEEE 802.11 (1999) Sec 8.2.3 --The WEP algorithm is applied to the frame body of an MPDU.].

With regard to dependent claim 16, Edwards in view of the IEEE teach the method of claim 1, wherein performing said encrypted WLAN communication further comprises receiving a data frame intended for said data frame decapsulation from a WLAN station and/or WLAN access point [IEEE 802.11 (1999) Sec 5.2.2.1].

With regard to dependent claim 17, Edwards in view of the IEEE teach the method of claim 1 wherein the step of performing said data frame decapsulation comprises obtaining cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation from a storage unit within the single-purpose hardware [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises WEP].

With regard to dependent claim 18, Edwards in view of the IEEE teach the method of claim 17, wherein said determining factor comprises a cipher protocol suitable for

performing the data frame decapsulation [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises WEP].

With regard to dependent claim 19, Edwards in view of the IEEE teach the method of claim 17, wherein said determining factor comprises a cryptographic key suitable for decrypting a data frame [IEEE 802.11 (1999) Sec 8.2.5 --cryptographic key is derived from IV which is associated with WEP].

With regard to dependent claim 20, Edwards in view of the IEEE teach the method of claim 16, wherein the step of performing said data frame decapsulation comprises decrypting at least part of the data frame [IEEE 802.11 (1999) Sec 8.2.3 --The WEP algorithm is applied to the frame body of an MPDU.].

With regard to dependent claim 26, Edwards in view of the IEEE teach the method of claim 1, wherein the step of performing said data frame encapsulation and/or decapsulation comprises generating cryptographic data suitable for encrypting or decrypting a data frame [IEEE 802.11 (1999) Sec 8.2.3 --generating keys, key sequence].

With regard to dependent claim 27, Edwards in view of the IEEE teach the method of claim 26, wherein the step of generating cryptographic data comprises generating authentication data suitable for encrypting a data frame in a manner specific to a WLAN station or decrypting a data frame encrypted in a manner specific to a WLAN station [IEEE 802.11 (1999) Sec 8.2.3 --ICV].

With regard to dependent claim 29, Edwards in view of the IEEE teaches the method of claim 1, wherein said encrypted WLAN communication is performed in a WLAN based

on the IEEE 802.11b standard [Edwards 3: 0038].

With regard to dependent claim 30, Edwards in view of the IEEE teach the method of claim 1, wherein said software-implemented instructions are executed on general-purpose hardware by driver software [Edwards Fig 4, Itm 20].

With regard to dependent claim 31, Edwards in view of the IEEE teach the method of claim 1. Edwards in view of the IEEE does not teach wherein said single-purpose hardware is operated periodically [Edwards 3: 0038 --802.11b defines RF to be 11 mhz.].

With regard to dependent claim 32, Edwards in view of IEEE teaches the method of claim 31.

Edwards in view of the IEEE does not teach wherein said single purpose hardware is operated periodically at 11 MHz.

Official Notice is taken that 802.11b defines WLAN to have a radio frequency centered at 11mhz.

It would have been obvious to one of ordinary skilled in the art at the time of invention to incorporate operation of the single purpose hardware at 11mhz as defined by the 802.11b. The suggestion/motivation for combining would have been to comply with the standard [Edwards 3: 0038 --802.11b].

Claims 46, 69, and 71 are rejected because all are similar matter to claim 1.

With regard to dependent claim 47, Edwards in view of the IEEE teach the single-purpose hardware device of claim 46, wherein said internal hardware components further comprise an internal memory for storing data frames intended for or resulting

from the data frame encapsulation or decapsulation [Edwards 4: 0049 --transmit queues].

With regard to dependent claim 48, Edwards in view of the IEEE teach the single-purpose hardware device of claim 47, wherein said internal memory comprises an arbitration unit for performing memory access control [Edwards 4: 0049 --transmit logic].

With regard to dependent claim 49, Edwards in view of the IEEE teach the single-purpose hardware device of claim 47, wherein said internal memory comprises a hash memory for storing cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation [Edwards 4: 0049 --transmit queues].

With regard to dependent claim 50, Edwards in view of the IEEE teach the single-purpose hardware device of claim 49, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation and/or decapsulation [IEEE 802.11 (1999) Sec 7.1.3.1 --comprises WEP].

With regard to dependent claim 51, Edwards in view of the IEEE teach the single-purpose hardware device of claim 49, wherein said determining factor comprises a cryptographic key suitable for encrypting or decrypting a data frame [IEEE 802.11 (1999) Sec 8.2.5 --cryptographic key is derived from IV and stored shared secret key which is associated with WEP].

With regard to dependent claim 52, Edwards in view of the IEEE teach the single-purpose hardware device of claim 47, wherein said internal hardware components further comprise a radio transceiver for receiving data frames from and/or transmitting

data frames to a WLAN station and/or WLAN access point [Edwards Fig 2, Itm 30].

With regard to dependent claim 53, Edwards in view of the IEEE teach the single-purpose hardware device claim 52, wherein said internal single-purpose hardware components comprise a cryptographic component for performing the data frame encapsulation and/or decapsulation [Edwards Fig 6: Itms 42, 50] and a MAC (Medium Access Control) component for communicating with the radio transceiver [Edwards Fig 6: Itm 24b].

With regard to dependent claim 54-57, Edwards in view of the IEEE teach: the cryptographic component and internal memory are arranged to communicate with each other [Edwards Fig 6: itm 42 coupled with 36/38]; cryptographic component and MAC component are arranged to communicate with each other [Edwards Fig 6: cryptographic component is part of MAC component]; MAC component and internal memory are arranged to communicate with each other [Edwards Fig 6: internal memory is part of MAC component]; and internal memory is arranged to communicate over the interface with external hardware components [Edwards Fig 6: internal memory is arranged to communicate over the interface, via the data encryption channel.].

Claims 59-61 are rejected because these are similar matter to claims 11, 26, and 27.

Regarding claim 72, Edwards in view of the IEEE teach the method as recited in claim 1, wherein the single-purpose hardware is a circuit dedicated for performing encapsulation and decapsulation without execution of any software instructions [Edwards Fig 4].

Regarding claim 73, Edwards in view of the IEEE teach the method as recited in claim 72, wherein the single-purpose hardware is coupled to receive plaintext data from the driver software, and wherein the single-purpose hardware is further coupled to provide decapsulated data to the driver software [Edwards Fig 4] [Edwards 4: 0050 -Examiner notes "unprocessed/raw packets" reading on plaintext data.].

Regarding claim 74, Edwards in view of the IEEE teach the single-purpose hardware device as recited in claim 53. Edwards in view of the IEEE does not explicitly teach wherein the single-purpose hardware device further includes a first multiplexer configured to select a communication path to the MAC component from either the internal memory or the cryptographic component, and further includes a second multiplexer configured to select a communication path to the internal memory from either the MAC component or the cryptographic component.

Official notice is taken that it is common and well known in the art to use multiplexers in for selecting communication paths.

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Edwards in view of the IEEE by incorporating multiplexers for selecting communication paths between the internal memory or the cryptographic component. The suggestion/motivation for combining would have been to select communication paths based on whether encryption/decryption of data frames needed for communication.

2. Claims 14-15, 21-25, 28, 33-35, 39-45, 62, and 65-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Edwards et al. [US 2004/0059825 A1],

hereinafter Edwards, and further in view of IEEE [IEEE 802.11 (1999)], and Cox [Cox 2003, NPL].

With regard to dependent claim 14, Edwards in view of the IEEE teach the method of claim 13. However, Edwards in view of the IEEE do not teach wherein the step of performing said data frame encapsulation comprises encrypting said integrity value. Cox teaches wherein the step of performing said data frame encapsulation comprises encrypting said integrity value [Cox (2003), Pg 20-21].

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Edwards in view of the IEEE to encrypt the integrity value. The suggestion/motivation for combining would have been to protect the authentication data along with the data payload.

With regard to dependent claim 15, Edwards in view of the IEEE and Cox teaches the method of claim 14, wherein the step of performing said data frame encapsulation comprises inserting the encrypted integrity value into one of the plurality of data frames [Cox (2003), Pg 20 --MIC is appended to the MSDU and is one of fragment MPDUs encapsulated by WEP].

With regard to dependent claim 21, Edwards in view of the IEEE and Cox teach the method of claim 20, wherein the data frame comprises an encrypted integrity value appropriate for verifying integrity of the data frame once said data frame decapsulation is completed, and the step of decrypting at least part of the data frame comprises decrypting the encrypted integrity value [Cox (2003), Pg 21 --MIC is one of fragment MPDUs. MPDU is part of MSDU data frame.].

With regard to dependent claim 22, Edwards in view of the IEEE and Cox teach the method of claim 21, wherein the step of performing said data frame decapsulation further comprises calculating the integrity value from at least part of the data frame except the encrypted integrity value [Cox (2003), pg 21 --WEP ICV, or MSDU recomputed MIC].

With regard to dependent claim 23, Edwards in view of the IEEE and Cox teach the method of claim 22, wherein the step of performing said data frame decapsulation further comprises calculating an integrity verification value indicating a difference between the decrypted integrity value and the calculated integrity value [Cox (2003), Pg 21 --output of comparator MIC and MIC'].

With regard to dependent claim 25, Edwards in view of the IEEE and Cox teach the method of claim 24, wherein performing said encrypted WLAN communication further comprises performing counter-measures according to said integrity verification value by executing software-implemented instructions, wherein said counter-measures are suitable for limiting the amount of information available to an illegitimate WLAN protruder frames [Cox (2003), Pg 19].

With regard to dependent claim 28, Edwards in view of the IEEE and Cox teach the method of claim 1, wherein said encrypted WLAN communication is performed based on the IEEE 802.11i security standard [Cox (2003), Pg 10].

With regard to dependent claim 33, Edwards in view of the IEEE and Cox teach the method of claim 31, wherein said data frame encapsulation and/or decapsulation is

performed according to the TKIP (Temporal Key Integrity Protocol) protocol [Cox (2003), Pg 20-21].

With regard to dependent claim 34, Edwards in view of the IEEE and Cox teach the method of claim 33, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing RC4 (Rivest's Cipher 4) encryption and/or decryption [Cox (2003), Pg 20-21 --WEP uses RC4].

With regard to dependent claim 35, Edwards in view of the IEEE and Cox teach the method of claim 34, wherein said RC4 encryption and/or decryption is performed by operating at least part of the single-purpose hardware [Edwards Fig 4].

With regard to dependent claim 39, Edwards in view of the IEEE and Cox teach the method of claim 34, wherein the step of performing said RC4 encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and said RC4 encryption and/or decryption to encrypt or decrypt one byte of the data frame.

Edwards in view of the IEEE and Cox does not teach encryption and decryption operations to be split over at least two operating periods of the single-purpose hardware.

Official notice is taken that it is common and well known in the art to have single-purpose hardware operations to be split over at least two operating periods to alleviate processing load over one operating period.

It would have been obvious to one of ordinary skilled in the art at the time of invention to have operations such as encryption and decryption to be split over at least to two

operating periods as it is common and well known in the art. The suggestion/motivation would have been to alleviate processing load over one operating period.

With regard to dependent claim 40, Edwards in view of the IEEE and Cox teach the method of claim 31, wherein said data frame encapsulation-and/or decapsulation is performed according to the CCMP (Counter-mode Cipher block chaining Message authentication code Protocol) protocol [Cox (2003), Pg 10].

With regard to dependent claim 41, Edwards in view of the IEEE and Cox teach the method of claim 40, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing CCMP-AES (Advanced Encryption Standard) encryption and/or decryption [Cox (2003), Pg 10].

With regard to dependent claim 42, Edwards in view of the IEEE and Cox teaches the method of claim 41, wherein the step of performing said CCMP-AES encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and said CCMP-AES encryption and/or decryption is performed by repeatedly performing a sequence of encryption or decryption steps on said part of the data frame [Cox (2003), Pg 10 --This is part of CCMP-AES].

With regard to dependent claim 43, Edwards in view of the IEEE and Cox teach the method of claim 42, wherein the step of performing the sequence of encryption or decryption steps comprises performing byte substitution using a plurality of cryptographic substitution boxes [Cox (2003), Pg 10 --AES comprises performing byte substitution using a plurality cryptographic substitution boxes.].

With regard to dependent claim 44, Edwards in view of the IEEE and Cox teach the method of claim 43, wherein the step of performing byte substitution on said part of the data frame comprises sequentially performing the byte substitution on a plurality of sub-parts of said part of the data frame [Cox (2003), Pg 10 --This is part of CCMP-AES].

With regard to dependent claim 45, Edwards in view of the IEEE and Cox teach the method of claim 42.

Edwards in view of the IEEE and Cox does not teach the step of performing the sequence of encryption or decryption operations to be split over at least two operating periods of the single-purpose hardware.

Official notice is taken that it is common and well known in the art to have single-purpose hardware operations to be split over at least two operating periods to alleviate processing load over one operating period.

It would have been obvious to one of ordinary skilled in the art at the time of invention to have operations such as encryption and decryption to be split over at least to two operating periods as it is common and well known in the art. The suggestion/motivation would have been to alleviate processing load over one operating period.

Dependent claim 62 is rejected using the same references as claims 33-35. Claim 62 is the apparatus for performing the methods of claims 33-35 combined.

Dependent claim 65 is rejected using the same references as claims 31 and 39. Claim 65 is the apparatus for performing the methods of claims 31 and 39 combined.

Dependent claim 66 is rejected using the same references as claims 40-43. Claim 66 is the apparatus for performing the methods of claims 40-43 combined.

Dependent claim 67 is rejected using the same references as claim 44. Claim 67 is the apparatus for performing the method of claim 44.

Dependent claim 68 is rejected using the same references as claims 31 and 45. Claim 68 is the apparatus for performing the methods of claims 31 and 45 combined.

3. Claims 36-38, and 63-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Edwards et al. [US 2004/0059825 A1], hereinafter Edwards, and further in view of IEEE [IEEE 802.11 (1999)], Cox [Cox 2003, NPL] and further in view of Campbell [Non-Patent Literature, November 2000].

With regard to dependent claim 36, Edwards in view of the IEEE and Cox teaches the method of claim 35, but does not explicitly disclose wherein said part of the single-purpose hardware has a tree structure [Tree structure is interpreted as a form of data structure.]

Campbell teaches a tree data structure that combines the advantages of searching performance of an ordered arrays, and the efficiency of insertion and deletion of data in a linked list data type structure for the storing and managing of data in a digital device.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Edwards in view of the IEEE and Cox to incorporate the use of the tree data structure of Campbell [a classic data structure well known in the art] for the storage and management of data involved in task/process execution. The suggestion/motivation for combining would have been to utilize the combined advantages of an ordered array and the efficiency of a linked list type data structure for storing and managing data in a digital device.

Claim 37 is rejected because it is the same method as claim 36, and wherein said RC4 encryption and/or decryption will inherently be performed by operating only a sub-part of the single-purpose hardware corresponding to the tree root, part of the tree leaves and the tree components interconnecting the tree root with said part of the tree leaves.

Claim 38 is rejected because it is the same method of claim 37, and wherein said sub-part of the single-purpose hardware will inherently correspond to the tree root, two of the tree leaves and the tree components interconnecting the tree root with said two of the tree leaves.

Dependent claim 63 is rejected using the same references and rationale as claims 36-37. Claim 63 is the apparatus for performing the methods of claims 36-37 combined.

Dependent claim 64 is rejected using the same reference and rationale as claim 38. Claim 64 is the apparatus for performing the method of claim 38.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Martin Jeriko San Juan/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432